(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 December 2003 (24.12.2003)

PCT

(10) International Publication Number
WO 03/107588 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/IB03/02337

(22) International Filing Date: 27 May 2003 (27.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02077422.0 17 June 2002 (17.06.2002) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LENOIR, Petrus, J.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TALSTRA, Johan, C.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DEN HEUVEL, Sebastiaan, A., F., A.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **STARING, Antonius, A., M.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.**; Philips Intellectual Property & Standards, Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

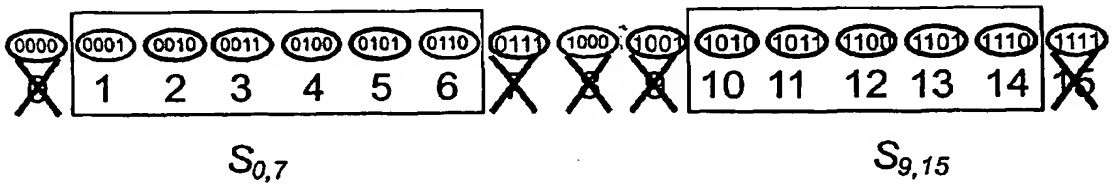
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR AUTHENTICATION BETWEEN DEVICES USING GROUP CERTIFICATES



(57) Abstract: In whitelist-based authentication, a first device (102) in a system (100) authenticates itself to a second device (103) using a group certificate identifying a range of non-revoked device identifiers, said range encompassing the device identifier of the first device (102). Preferably the device identifiers correspond to leaf nodes in a hierarchically ordered tree, and the group certificate identifies a node (202-207) in the tree representing a subtree in which the leaf nodes correspond to said range. The group certificate can also identify a further node (308, 310, 312) in the subtree which represents a sub-subtree in which the leaf nodes correspond to revoked device identifiers. Alternatively, the device identifiers are selected from a sequentially ordered range, and the group certificate identifies a subrange of the sequentially ordered range, said subrange encompassing the whitelisted device identifiers.

WO 03/107588 A1

INTERNATIONAL SEARCH REPORT

Interna d Application No
PCT/IB 03/02337

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	WO 00 68762 A (SUN MICROSYSTEMS INC) 16 November 2000 (2000-11-16) abstract page 5, line 4 - line 17 page 6, line 3 -page 7, line 2 page 9, line 1 - line 7 page 10, line 21 - line 24 page 16, line 9 - line 16 figure 7	1,5-7, 9-12 2,3 4,8
A	WO 02 41527 A (LORAL SPACE SYSTEMS INC) 23 May 2002 (2002-05-23) abstract figure 1	5,6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 October 2003	17/11/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern d Application No
PCT/IB 03/02337

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 130 844 A (SONY CORP) 5 September 2001 (2001-09-05) abstract figure 1	10,11
Y	D. NAOR, M. NAOR, J. LOTSPIECH: "Revocation and Tracing Schemes for Stateless Receivers" ADVANCES IN CRYPTOLOGY, CRYPTO'01, 24 February 2001 (2001-02-24), pages 41-62, XP002259238 cited in the application	2,3
A	abstract page 45, line 26 -page 53, line 29 figures 2,3	8
X	US 5 220 604 A (KAUFMAN CHARLES W ET AL) 15 June 1993 (1993-06-15)	1,7,9,12
A	abstract column 9, line 66 -column 11, line 11 figure 4A	2-6,8, 10,11
X	US 2001/049787 A1 (FUKUDA KENICHI ET AL) 6 December 2001 (2001-12-06)	1,9,12
A	abstract page 5, paragraph 108 -page 6, paragraph 119	2-8,10, 11
A	DE 195 11 298 A (DEUTSCHE TELEKOM AG) 2 October 1996 (1996-10-02) abstract figure 1	4

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter al Application No
PCT/IB 03/02337

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0068762 A	16-11-2000	AU 4502700 A	21-11-2000
		EP 1177492 A1	06-02-2002
		WO 0068762 A1	16-11-2000
WO 0241527 A	23-05-2002	AU 1139702 A	27-05-2002
		WO 0241527 A1	23-05-2002
EP 1130844 A	05-09-2001	JP 2001320356 A	16-11-2001
		EP 1130844 A2	05-09-2001
		US 2001034834 A1	25-10-2001
US 5220604 A	15-06-1993	NONE	
US 2001049787 A1	06-12-2001	JP 2001326632 A	22-11-2001
		DE 10124111 A1	04-07-2002
DE 19511298 A	02-10-1996	DE 19511298 A1	02-10-1996